

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

|                          |   |  |
|--------------------------|---|--|
| UNITED STATES OF AMERICA | ) |  |
|                          | ) |  |
|                          | ) |  |
| v.                       | ) | Criminal Action Nos. 09-273-03 and 10-021-02 |
|                          | ) |  |
| ERIN HOUSE,              | ) |  |
| Defendant.               | ) |  |
|                          | ) |  |

**MEMORANDUM OPINION**

**CONTI, Chief District Judge.**

Pending before the court are motions to dismiss the indictment or to suppress evidence, and for a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978) filed by Erin House (“defendant”). (ECF Nos. 313, 333, and 601.)<sup>1</sup> Defendant contends that the government conducted illegal, warrantless searches of his tractor truck, a co-defendant’s cellular telephone, and his own cellular telephone during the investigation of this case, warranting suppression of the evidence gathered. Defendant further contends that the indictments against him should be dismissed because the government engaged in discovery misconduct, including failing to disclose exculpatory evidence and altering evidence that was disclosed to him. For the reasons set forth below, defendant failed to establish that he is entitled to relief under any legal doctrine and his motions will be denied.

---

<sup>1</sup> All citations to the record will refer to the docket of the first-filed case, Criminal Action Number 09-273, unless otherwise specified.

## **I. FACTUAL AND PROCEDURAL BACKGROUND**

On September 15, 2009, a federal grand jury in the Western District of Pennsylvania returned a one-count indictment charging defendant, and seven co-defendants, with conspiracy to possess with the intent to distribute and to distribute five kilograms or more of cocaine in violation of 21 U.S.C. §§ 841(a)(1), 841(b)(1)(A)(ii), and 846. (ECF No. 1.) On September 18, 2009, defendant pleaded not guilty to this charge. (ECF No. 21.)

A five-count superseding indictment was returned on December 8, 2009. (ECF No. 145.) Count One charged defendant and the same seven co-defendants with the same drug trafficking conspiracy charged in the original indictment, although contending that the conspiracy began a month earlier than charged in the original indictment. (Id.) The first superseding indictment's remaining four counts were charged against certain of defendant's co-defendants, but not against defendant. (Id.) Defendant pleaded not guilty to Count One of the first superseding indictment on December 15, 2009. (ECF No. 160.) In a January 13, 2010 motion to compel, defendant stated his intention to file various motions to suppress based upon the government's alleged unlawful interception of push-to-talk communications to and from cellular telephone devices, and an alleged warrantless search of his tractor truck. (ECF No. 192 at 2-3.) Defendant's first motion to suppress was filed on August 30, 2010. (ECF No. 313.) Defendant was represented by counsel when that motion was filed, but has proceeded pro se, with the assistance of stand-by counsel, since June 2012. (ECF Nos. 561, 563.)

On August 22, 2012, a federal grand jury in the Western District of Pennsylvania returned a two-count, second superseding indictment charging defendant and co-defendant Michael Dwayne Blackwell (“Blackwell”), at Count One, with the same drug trafficking conspiracy charged in the two previous indictments. (ECF No. 575.) Count Two charged Blackwell with possession of firearms in connection with the drug trafficking conspiracy. (*Id.*) Defendant’s remaining six co-conspirators were not named in the second superseding indictment because they had each pleaded guilty to the drug trafficking conspiracy before the second superseding indictment was returned. (ECF Nos. 371, 379, 412, 415, 418, and 431.) Defendant moved to dismiss the second superseding indictment, and pleaded not guilty on October 11, 2012. (ECF Nos. 587, 601, 602.) Blackwell also pleaded not guilty to the charges brought against him in the second superseding indictment, but changed his plea to guilty on Count One (the drug trafficking conspiracy) on November 10, 2014. (ECF Nos. 620, 775.) Blackwell was sentenced by this court on February 26, 2015. (ECF No. 816.) Count Two of the second superseding indictment, and all charges against Blackwell in the original and first superseding indictment were dismissed on the motion of the government following sentencing. (*Id.* at 1; ECF Nos. 817, 818.) Prior to his guilty plea, Blackwell joined the motions currently advanced by defendant, but for present purposes the court refers to the motions as defendant’s motions, not defendant’s and Blackwell’s motions.

Between the filing of the first and second superseding indictments, defendant and co-defendant Blackwell asked the United States District Court for the Northern District of Ohio to transfer a criminal case pending against them in that court to the Western District of Pennsylvania. United States v. House, et al., 09-436 (N.D. Oh. Oct. 14, 2009); (10-021, ECF No. 1 at 1.) The charges brought against defendant in Ohio involved interstate travel for the purposes

of engaging in drug trafficking, and possession with the intent to distribute cocaine and heroin. (10-021, ECF No. 1-1.) The Ohio case, to the extent charged against defendant and Blackwell, was transferred to this court, assigned Criminal Action Number 10-021, and consolidated with Criminal Action Number 09-273. (09-273, ECF Nos. 214, 232; 10-021, ECF No. 7.) At defendant's request, all motions filed in the 09-273 case were adopted for purposes of the related 10-021 case. (10-021, ECF Nos. 18, 20.)

As stated previously, defendant filed the first of his motions to suppress, to dismiss, or for a Franks hearing on August 30, 2010, (ECF No. 313), and most recently requested leave to supplement his motions on September 28, 2013, (ECF Nos. 718, 723, and 730). Defendant filed numerous other supplements and motions to supplement in the interim, (ECF Nos. 333, 691), as well as other motions, including for discovery, to dismiss, to compel, and to suppress other evidence (see e.g., ECF Nos. 601, 711, and 724, and 10/16/2013 Text Order; 10-021, ECF Nos. 25, 29, and 30). The government filed written responses to many of defendant's motions, and addressed others at hearings before the court. (see e.g., ECF Nos. 332, 401, 405, 461, 727, 733, and 734.)

The motions to suppress or dismiss that are ripe for decision by the court are ECF Nos. 313, 333 and 601 in Criminal Action Number 09-273, and ECF No. 25 in Criminal Action Number 10-021.<sup>2</sup> The grounds on which defendant seeks relief in connection with those

---

<sup>2</sup> The court finds no indication in the record that defendant joined Blackwell's motion to suppress evidence recovered from the search of a residence in Downey, California. (ECF No. 713.) That motion, which concerned the seizure of firearms to which Blackwell was objecting, is moot in light of Blackwell's guilty plea and judgment. Defendant was granted the relief requested in the pending motions for leave to supplement previously-filed motions, and to compel discovery, filed at ECF Nos. 691, 711, and 718, by virtue of the filings that defendant has made, the evidence that the government has presented and produced, and the hearings that the court has held in this case. Those motions are moot.

motions, however, are confined to the evidence relied upon and arguments made by defendant in his proposed findings and conclusions.<sup>3</sup>

Hearings were held on defendant's motions on April 7, 2010, October 18, 2010, June 22, 2011, December 19, 2011, April 30, 2012, November 16, 2012, December 10, 2012, August 20, 2013, December 11, 2013, December 12, 2013, January 6, 2014, and April 25, 2014. (09-273, ECF Nos. 259, 356, 458, 537, 556, 769, 640, 770, 822, 821, and 756, respectively; 10-021, ECF No. 164 (12/12/13 hearing).) During these hearings, the court admitted evidence and heard testimony from FBI Special Agents Sandra Maier ("SA Maier"), Tanya Evanina ("SA Evanina"), and Christopher Kopp ("SA Kopp"), Police Officers Richard Menges ("Menges") and Scott Payne ("Payne"), Sprint Communications representatives Joseph Trawicki ("Trawicki"), Thomas Koch ("Koch"), and Marc Grovier ("Grovier"), Henry Joseph Hodor ("Hodor"), and Ben Levitan ("Levitan"), an expert proffered by defendant.

At the final evidentiary hearing, the court established a tentative schedule for the parties to submit proposed findings of fact and conclusions of law after the transcripts of all hearings were filed. (4/25/2014 Minute Entry.) Defendant objected to the briefing schedule once it was set by the court on the ground that he had not yet received full copies of all transcripts. (7/21/2014 Minute Entry; ECF Nos. 765, 766.) The court thereafter amended the scheduling order, providing more time for defendant to obtain the needed transcripts and submit his

---

<sup>3</sup> By way of example to demonstrate the court's point, although Blackwell moved to suppress the search warrant issued for the Miles Road property in Ohio on the ground that it was an improper anticipatory warrant (10-021, ECF No. 25), defendant includes no evidence or argument about this issue in his proposed findings and conclusions. Therefore, although defendant joined Blackwell's motion, (10-021, ECF No. 29, 30), the court will not address that issue, or afford defendant relief on that basis. The same analysis applies to any argument made in a motion or brief by defendant or Blackwell, but not pursued in defendant's proposed findings and conclusions. Defendant was advised that the court would proceed in this manner and rely upon his proposed findings and conclusions as framing the issues that were still being pursued by this defendant and were ripe for decision. (ECF No. 756 at 123-24.)

proposed findings and conclusions. (ECF No. 768.) Defendant timely filed his proposed findings and conclusions on November 24, 2014. (ECF No. 779.) The court granted a thirty-day extension to the government to file its proposed findings and conclusions, and after defendant objected to the extension, specifically found the extension to be necessary and appropriate, and deemed all time excludable delay under the Speedy Trial Act, 18 U.S.C. § 3161. (ECF Nos. 793, 794, 799, 800, 805, 806.)

Pursuant to the court's amended scheduling order, defendant's reply to the government's submission was due on March 9, 2015. (ECF No. 794.) That filing was received by the Clerk of Court on March 10, 2015, which this court deems timely given the need for defendant to submit the document, by mail, for manual docketing. (ECF No. 820.) Although the record should have been closed as of March 10, 2015, in his reply, defendant objected to the government's submission of three new evidentiary exhibits with its proposed findings and conclusions. (Id. at 1-4, 40-41.) Based upon defendant's objection, the court entered an order on that same date, March 10, 2015, directing the government to respond to defendant's objection by March 24, 2015, and setting a hearing on defendant's objection for April 15, 2015. (ECF No. 823.) In that order, the court set forth its reasons for finding the delay related to defendant's objection excludable under the Speedy Trial Act. (Id., citing 18 U.S.C. §§ 3161(h)(7)(A) and (h)(1)(D).)

The government filed its response to defendant's objection on March 24, 2015. (ECF No. 825.) On March 27, 2015, after reviewing the government's response, the pertinent portions of the record in light of that response, and defendant's objections, the court entered an order directing the government to either file a motion to reopen the record or to withdraw the exhibits to which defendant was objecting no later than April 9, 2015. (3/27/2015 Minute Entry.)

On April 9, 2015, the government filed a motion to reopen the record. (ECF No. 832.) The court heard argument on the government's motion, and defendant's objections, at the April 15, 2015 hearing. (ECF No. 841.) The parties agreed at the hearing that Government Exhibit 31 should be admitted into the record, but disputed whether the court should consider the other two new government exhibits. (Id. at 9.) The court issued a written opinion denying the government's motion to reopen the record, due primarily to the prejudice that would result from admitting the government's new evidence. (ECF No. 842.)

Upon consideration of the parties' written submissions, and the evidence and testimony presented at the hearings on defendant's motions, the court makes the following findings of fact and conclusions of law.

## **II. FINDINGS OF FACT**

### **A. General Background Information**

FOF 1) The motions to suppress or dismiss that are ripe for decision by the court are ECF Nos. 313, 333 and 601 in Criminal Action Number 09-273, and ECF No. 25 in Criminal Action Number 10-021. Hearings were held on defendant's motions on April 7, 2010, October 18, 2010, June 22, 2011, December 19, 2011, April 30, 2012, November 16, 2012, December 10, 2012, August 20, 2013, December 11, 2013, December 12, 2013, January 6, 2014, and April 25, 2014. (09-273, ECF Nos. 259, 356, 458, 537, 556, 769, 640, 770, 822, 821, and 756, respectively; 10-021, ECF No. 164 (12/12/13 hearing).)

FOF 2) The investigation leading to these criminal charges consisted of physical surveillance of the defendants, review of domestic flight records, monitoring cellular telephone activity, and intercepting the content of cellular telephone conversations. (ECF No. 537 at 42-43,

51; ECF No. 640 at 23-26, 60-61; ECF No. 821 at 20, 74-75; Gov. Exs. 1, 2, 3, and 24; Def. Exs. F, Z.)

**B. Cellular Telephone Technology and Terminology**

FOF 3) A Nextel cellular telephone device can be used to engage in both traditional, open-line telephone communications and push-to-talk (“PPT”) communications. (ECF No. 537 at 88-89.) A PTT communication is sometimes referred to “direct connect.” PTT is a communication technique unique to Nextel and requires the use of a Nextel cellular telephone device operating on Nextel’s iDEN network. (ECF No. 537 at 88, 98-99, 100-01, 112, 114; ECF No. 556 at 73-75.)

FOF 4) For a Nextel cellular telephone, both traditional telephone and PTT communications are carried on the iDEN network, a network that was created before Nextel merged with Sprint. (ECF No. 537 at 82, 85-86, 94; ECF No. 556 at 97, 111-13, 121-22.) Although a PTT communication follows a different technological path, or protocol, it is carried on the same iDEN network and uses the same Nextel cellular telephone device as a traditional telephone communication. (ECF No. 556 at 96, 111-13, 116.) Sprint utilizes the CDMA network. (ECF No. 537 at 81-82, 118; ECF No. 556 at 111-13.) Even after Sprint and Nextel merged, they retained their separate network technology. (ECF No. 537 at 82; ECF No. 556 at 111-12.) Only a legacy Nextel cellular telephone device operating on the legacy Nextel iDEN network can engage in PTT communications. (ECF No. 537 at 81-82.)

FOF 5) In order for a Nextel cellular telephone device to initiate a traditional telephone communication, the device communicates with the cell tower with the strongest signal, which is typically the closest tower, by radio frequency, which tower then communicates with the nearest available switching station, or “switch,” which then, ultimately, passes the call off to



the switching station where the recipient of the communication is located. (ECF No. 537 at 91-92; ECF No. 756 at 8-11.) The same process is used when a Nextel cellular telephone engages in a PTT communication, through the use of slightly different technology, but using the same iDEN network and the same system of cell towers and switches. (ECF No. 537 at 84-86, 93-94.)

FOF 6) Defendant and Blackwell each possessed Nextel cellular telephone devices when they were arrested. (ECF No. 537 at 82; ECF No. 779 at 4 & nn.21-22; Def. Ex. OO.)

FOF 7) When engaging in a traditional telephone communication using any cellular telephone, the line remains open and both parties can talk over it at any time, or even at the same time, until one participant hangs up. (ECF No. 556 at 52-53.) A PTT conversation, however, is akin to a walkie-talkie communication. It is a one-way communication in which one person connects the line by pressing a button on the side of his or her cellular telephone device, speaks, and disconnects the line by releasing the button, and the other person responds by connecting the line by pressing a button on the side of his or her cellular telephone device, speaking, and disconnecting the line by releasing the button. (ECF No. 537 at 93-94; ECF No. 556 at 50-53); see United States v. Shaw, 874 F.Supp.2d 13, 15-16 & n.4 (D. Mass. 2012).

FOF 8) To initiate a traditional telephone communication a ten-digit number is dialed, in the familiar format of a three-digit area code, followed by a three-digit number, a hyphen, and a four-digit number. (ECF No. 537 at 119.) This number will be referred to as the “traditional telephone number.”

FOF 9) To initiate a PTT conversation a multi-digit number, called an Urban Fleet Member ID, or “UFMI,” which consists of three groups of numbers of varying lengths, separated by two asterisks, is dialed. (ECF No. 537 at 98; ECF No. 556 at 71-72; ECF No. 821 at 100-01.) This number will be referred to as the “UFMI/PTT number.”

FOF 10) A Nextel cellular telephone has two electronic identifiers: an IMSI number, and an ESN number. (ECF No. 537 at 86-89; ECF No. 556 at 7-8, 14.)

FOF 11) An “IMSI number” is the International Mobile Subscriber Identity number, which is a multi-digit number assigned to the SIM card found in a Nextel cellular telephone upon activation. A Nextel cellular telephone cannot be used to engage in either traditional telephone communications or PTT communications without a SIM card inserted into the cellular telephone device. (ECF No. 537 at 86-89; ECF No. 556 at 14-15, 88.)

FOF 12) The IMSI number placed on or assigned to a SIM card is immutable; the IMSI number will not change unless or until it is reprogramed. (ECF No. 537 at 88-89.) The SIM card can be removed from a particular cellular telephone device and placed into a different cellular telephone device and the IMSI number will not change, and the same traditional telephone number and the same UFMI/PTT number could be used. (ECF No. 537 at 88-89.) By the same token, the SIM card can remain in the same cellular telephone device, but the user can have the traditional telephone number or the UFMI/PTT number changed. (ECF No. 537 at 83-89.) In this instance, again, the SIM card will retain the same IMSI number. For this reason, the IMSI number is viewed as the best identifier of an individual’s cellular telephone communications. (ECF No. 537 at 87-90, 102; ECF No. 556 at 123-24.)

FOF 13) An “ESN number” is the Electronic Serial Number, which is a unique, multi-digit identifier assigned to the cellular telephone device itself. (ECF No. 556 at 7-8.)

FOF 14) Call Detail Records (“CDR”) are compiled by a cellular provider, such as Sprint/Nextel, for billing purposes, using systems and personnel that are unrelated to those that implement government surveillance orders. (09-273, ECF No. 756 at 8; 10-021, ECF No. 164 at 150-51, 164-65.) CDR capture only calls that achieve a network connection, and are time

stamped when that connection is achieved. (09-273, ECF No. 756 at 11, 13, 25; 10-021, ECF No. 164 at 164, 166.) The clocks used by the CDR systems and the government surveillance systems are located in different time zones and are not synchronized. (09-273, ECF No. 756 at 24; 10-021, ECF No. 164 at 167-68.)

FOF 15) Contemporaneous cell tower site location information indicates the cell tower that an incoming or outgoing communication is hitting off of at the start of a communication and the end of a communication. (ECF No. 537 at 144-45.) The information provided gives a broad or generalized location, such as “Pittsburgh, Pennsylvania” or “Southern California,” and reflects the location of the cell tower being used to connect a user’s cellular telephone device to the cellular network. Contemporaneous cell tower site location does not reveal the precise location of the cellular telephone device itself. (ECF No. 537 at 25.)

FOF 16) “Pinging” provides more precise information about the physical location of a cellular telephone device. A cellular telephone device can be “pinged” by manually sending an electronic signal to the target device, or by setting up a system by which an electronic message is sent directly to the device at regular intervals. (ECF No. 537 at 152-53.) The information provided reflects the GPS position of the cellular telephone device itself; it does not indicate the cell towers with which the device is communicating. (ECF No. 537 at 25-26, 144-45.)

FOF 17) “The term ‘pen register’ means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic

communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.” 18 U.S.C. § 3127(3). In other words, a pen register records the outgoing communications from a cellular telephone device and is not the same thing as a CDR. Id.; (ECF No. 537 at 139.)

FOF 18) “The term ‘trap and trace device’ means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.” 18 U.S.C. § 3127(4). In other words, a trap and trace records the incoming communications of a cellular telephone device. (ECF No. 537 at 139.)

FOF 19) A pen register and trap and trace, referred to collectively herein as a “pen/trap,” must be activated at particular physical locations, or switches, where a user is expected to engage in communications using his cellular telephone device. (ECF No. 537 at 147; ECF No. 756 at 13-17, 25, 57-58.) Law enforcement directs the service provider to activate the pen/trap in those markets where the subscriber is likely to be located. (ECF No. 537 at 147; ECF No. 756 at 13-16, 25; see e.g., Gov. Ex. 28 (listing geographic markets in which the pen register on defendant’s Nextel cellular telephone device would be implemented).) The switch associated with the location where the subscriber registered the cellular telephone, or the “home switch,” and certain oft-used switches will be activated for the collection of data. (ECF No. 537 at 147; ECF No. 756 at 13-16, 25.) If a switch is not activated for surveillance, law enforcement will not receive information about any outgoing calls placed from that area. (09-273, ECF No. 537 at

147; ECF No. 756 at 13-14, 16-17, 57-58; 10-021, ECF No. 164 at 192). Information about all incoming calls will be gathered even if the user is in a market that has not been activated for surveillance because incoming calls are always routed through the home switch first, and the home switch is always activated. (ECF No. 756 at 16-17, 58-59.)

FOF 20) A pen/trap does not intercept the content of any communications. 18 U.S.C. § 3127(3) & (4). A wiretap does. 18 U.S.C. §§ 2510-20.

FOF 21) Pursuant to Title III of The Omnibus Crime Control Act of 1968, the interception of wire, oral, or electronic communications is prohibited, except upon approval of an application made by the Attorney General to a Federal judge of competent jurisdiction. 18 U.S.C. §§ 2510-2520; 18 U.S.C. § 2516.

FOF 22) “‘Wire communication’ means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.” 18 U.S.C. § 2510(1). “‘Aural transfer’ means a transfer containing the human voice at any point between and including the point of origin and the point of reception.” 18 U.S.C. § 2510(18).

FOF 23) “‘Oral communication’ means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.” 18 U.S.C. § 2510(2).

FOF 24)        “‘Electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: (a) any wire or oral communication; (b) any communication made through a tone-only paging device; (c) any communication from a tracking device (as defined in [18 U.S.C. § 3117]); or (d) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.” 18 U.S.C. § 2510(12). Emails and text messages are examples of electronic communications. (ECF No. 537 at 106-07.)

FOF 25)        Like pen/traps, wiretaps must be activated or provisioned in certain locations where law enforcement expects a target to be using his or her cellular telephone device. See FOF 19; (ECF No. 537 at 147-48; see e.g., Def. Exs. A, B (listing “market areas for implementation” for a wiretap)).

FOF 26)        When Sprint/Nextel receives an order to intercept wire communications associated with an ISMI number, it provides law enforcement with both traditional telephone communications and PTT communications, unless it is specifically instructed otherwise, which law enforcement sometimes does in order to reduce the cost of the wiretap. (ECF No. 537 at 78-80, 87-91, 99-103, 109.) The IMSI number is what Sprint/Nextel “taps” or intercepts pursuant to a Title III wiretap order. (ECF No. 537 at 90, 99, 102.)

FOF 27)        Although defendant’s expert witness, Levitan, testified that a different IMSI is assigned each time a PTT communication occurs, making it impossible to implement a surveillance or wiretap order using the IMSI number, his explanation was not credible and was directly contradicted by every Sprint/Nextel representative who testified. (ECF No. 556 at 83,

94-108.) Levitan never implemented a wiretap order on behalf of law enforcement. (ECF No. 556 at 35-37.) The Sprint/Nextel representatives, who have first-hand experience in provisioning and implementing surveillance systems for law enforcement pursuant to orders authorizing pen/traps and wiretaps, testified that the ISMI is immutable and inextricably linked to the SIM card found in a Nextel cellular telephone device, without which the device will not operate, whether for traditional telephone communications or PTT communications. (ECF No. 537 at 87, 102, 118.) Those representatives testified consistently and credibly that the PTT communications from a cellular telephone device could be intercepted if the IMSI number is provided by law enforcement. FOF 26.

### **C. Surveillance of Blackwell's Cellular Telephone**

FOF 28) Blackwell's cellular telephone is referred to as Target Telephone #4 ("TT4") in these proceedings. (Def. Ex. C.) TT4 was a Nextel device operating on the iDEN network. (ECF No. 537 at 81-83; Def. Exs. C, G, PP.) That cellular telephone device was assigned the traditional telephone number (323) 208-0259, the IMSI number 316010154698906, and the UFMI/PTT number 124\*493\*1757. (ECF No. 820 at 2; Def. Ex. C.)

FOF 29) On May 26, 2009, then-Magistrate Judge Cathy Bissoon, at No. 09-294M, authorized the installation and use of a pen/trap on a cellular telephone being used by an unknown individual "believed to be Jeff Sayles' cocaine supplier," and now known to be Blackwell. (Def. Ex. PP at 31.) The judge also authorized the collection of call detail records and contemporaneous cell tower site location information for that telephone. (Id.) The telephone was identified as "Sprint cellular telephone number (323) 208-0259, a cellular telephone subscribed to Camps KC, 12617, Crenshaw Blvd., Hawthorne, California 90250, IMSI 316010154698906 (and any replacement telephone number(s) obtained by the same subscriber(s)

or on the cellular telephone bearing the same IMSI during the period covered by the court order).” (Def. Ex. PP at 30-31.)

FOF 30) The order authorizing the pen/trap for Blackwell’s phone, by its terms, would automatically expire sixty days from the date on which it was signed, or on July 25, 2009. (Def. Ex. PP at 32-34.)

FOF 31) Although the application, affidavit, and court order for the pen/trap on TT4 did not refer to direct connect or PTT communications, the service order stated that information about PTT communications should be provided to the FBI. (Def. Ex. PP at 36.) The service order is signed by the judge and then sent to the cellular provider directing it to implement the court-authorized surveillance. (Id.)

FOF 32) On July 8, 2009, District Judge David Cercone, at Misc. No. 09-135(b), authorized the interception of wire communications to and from TT4. (Def. Ex. C.) The Title III wiretap order listed the traditional telephone number ending in -0259, the IMSI number ending in -8906, and the Camps KC subscriber information, as set forth in the order signed by Magistrate Judge Bissoon approximately six weeks earlier. (Id.) The order stated that interception could continue even if either the IMSI number or traditional phone number was changed. (Id.) The order signed by Judge Cercone, by its terms, would automatically expire no more than thirty days from the date on which it was signed, or on August 6, 2009. (Id.)

FOF 33) The Authorization for Interception Order Memorandum for TT4 signed by a designated official of the Attorney General of the United States on July 7, 2009, lists the traditional telephone number associated with TT4, as well as the Camps KC subscriber information, and authorizes the interception of any wire communications “accessed through IMSI number 316010154698906.” (Def. Ex. YY.) The authorization states that it “is intended to



apply not only to the target telephone numbers listed above, but also to any other telephone numbers or telephones accessed through the above-referenced IMSI number, and to any other IMSI number accessed through the target telephone number referenced above.” (Id.)

FOF 34) The Attorney General’s authorization, and the application and affidavit submitted to and the orders signed by Judge Cercone do not specifically refer to direct connect or PTT communications. (Def. Ex. C.)

FOF 35) The FBI instructed Sprint/Nextel to initiate this wiretap for TT4 by faxing the service order and a form called a “CALEA Coversheet” to Sprint/Nextel on July 8, 2009. (Def. Ex. A.) A second CALEA Coversheet was faxed to Sprint/Nextel on July 9, 2009. (Def. Ex. B.) Whereas the first CALEA Coversheet filled in the blanks for a surveillance start date and a surveillance termination date for traditional cellular telephone communications, the second CALEA Coversheet filled in the blanks for a surveillance start date and a surveillance termination date for both traditional cellular telephone communications and “Dispatch,” or PTT, communications. (Def. Ex. B.) The second CALEA Coversheet specified the same surveillance start date for both PTT and traditional telephone communications as was specified for the traditional cellular telephone communications on the first CALEA Coversheet, i.e., July 8, 2009. (Id.)

FOF 36) A second CALEA Coversheet was necessary because although Sprint/Nextel considers an order authorizing the interception of wire communications from a cellular telephone device identified by its IMSI number to authorize the interception of both traditional telephone and PTT communications, the first CALEA Coversheet did not provide a date on which the interception of PTT communications should begin. (ECF No. 537 at 78-80, 90-91, 99-103; ECF No. 556 at 3-6; Def. Exs. A, B.) Because law enforcement will sometimes ask

the cellular service provider to intercept less than all the communications that are authorized due to financial constraints, Sprint/Nextel officials seek clarification before setting up the surveillance system if the CALEA Coversheet does not indicate that all authorized interception types should be delivered to law enforcement. (ECF No. 537 at 107-10.)

FOF 37) In this case, a surveillance start date was not specified for PTT communications on the July 8, 2009 CALEA Coversheet because the FBI was not aware at that time that Blackwell used TT4 to engage in PTT communications. (ECF No. 556 at 3-9.) The FBI became aware of this usage when a Sprint/Nextel technician contacted the case agent to seek clarification with respect to whether the FBI wished to pay for the interception of both traditional telephone and PTT communications. (ECF No. 537 at 108-10; ECF No. 556 at 3-9, 136-37, 142-43.) SA Maier's and Sprint representative Trawicki's testimony about this chronology of events was consistent and credible.

FOF 37(a) The Vaughn Index submitted by defendant with his proposed findings of fact and conclusions of law does not draw this chronology of events into question, as defendant contends. (ECF No. 779 at 5 & nn. 33-34.) The index reflects a communication, on July 13, 2009, between the Attorney General's office, and the United States Attorney about "the scope of the AAG's review of the AUSA's Title III request." (Def. Ex. QQ at 33.) This entry is ambiguous and is not probative of defendant's assertion that the government was not authorized to intercept TT4's PTT communications until July 13, 2009.

FOF 37(b) The fact that the May 26, 2009 service order authorizing the pen/trap on TT4 refers to direct connect communications does not draw this chronology of events into question, as defendant contends. See FOF 29; (Def. Ex. PP at 36; ECF No. 779 at 5

nn.27-30.) Although the May 26, 2009 service order specifically references direct connect communications, there is no dispute in the record that the application and affidavit submitted by SA Maier in support of that service order do not reference PTT communications. See FOF 31. There is likewise no dispute that SA Maier was not personally aware that Blackwell used TT4 to engage in PTT communications at the time she prepared those documents. See FOF 37. The explicit reference to direct connect communications in the May 26, 2009 service order, therefore, does not controvert SA Maier's testimony. Based upon this record, the explicit reference to direct connect communications in the May 26, 2009 service order is not probative of defendant's assertion that the government knew that TT4 was used to engage in PTT communications when the first wiretap order was signed on July 8, 2009, but failed to specifically list PTT communications in the paperwork associated with that wiretap order because the interception of such communications was not authorized.

FOF 38) Judge Cercone, at Misc. No. 135(c), signed a second order authorizing the interception of wire communications to and from TT4 on August 5, 2009. (Def. Exs. D, Z.) This order, by its own terms, would automatically expire thirty days after it was signed. (Def. Ex. D at 5.) Unlike the order signed by Judge Cercone on July 8, 2009, this service order specifically stated that it applied to the "direct connect/dispatch services' feature of this Sprint telephone." (Id. at 2.) SA Maier's affidavit filed in support of this second wiretap order recounted the content of various conversations, which she specifically identified as PTT communications, that had been intercepted over TT4 pursuant to the Title III wiretap order signed by Judge Cercone on July 8, 2009. (Def. Ex. Z (e.g., ¶¶ 19, 21).)

**D. Surveillance of Defendant's Cellular Telephone**

FOF 39) Defendant's cellular telephone was assigned the traditional telephone number (562) 307-2726, the IMSI number 316010017050612, and the UFMI/PTT number 124\*143819\*1. (ECF No. 820 at 12.) Defendant's cellular telephone was a Nextel device operating on the iDEN network. (ECF No. ECF No. 537 at 138; ECF No. 820 at 12.)

FOF 40) On July 15, 2009, Magistrate Judge Robert Mitchell, at No. 09-371M, authorized the installation and use of a pen/trap on a cellular telephone identified by the traditional telephone number (562) 307-2726 and the ESN 000819330761330, which was described as a device belonging to defendant. (Gov. Ex. 1 (see also Def. Ex. E).) No UFMI/PTT or IMSI numbers were listed, and no mention was made about whether the device was used to engage in PTT communications. In addition to the pen/trap, the collection of contemporaneous cell tower site location information was authorized. (Id.; ECF No. 537 at 25.) The order would automatically expire sixty days from the date on which it was signed, or on September 14, 2009. (Id.)

FOF 41) On that same day, Magistrate Judge Mitchell, at No. 09-372M, issued an order authorizing the government to ping defendant's cellular telephone device. (Gov. Ex. 2.) This order, by its terms, would automatically expire thirty days from the date on which it was signed, or on August 14, 2009. (Id.; ECF No. 537 at 41.)

FOF 42) On August 18, 2009, Magistrate Judge Lenihan, at No. 09-444M, signed an order authorizing the government to ping defendant's cellular telephone device for another thirty days. (Gov. Ex. 3.) No ping order was in place for defendant's device between August 14, 2009 and August 18, 2009, but the pen/trap order, which also authorized the collection of contemporaneous cell tower site location information, remained in full force and effect during

this time period. (Gov. Exs. 1 and 2.) A Title III wiretap order was never issued for defendant's cellular telephone device.

**E. Alleged Illegal Surveillance of Cellular Telephones**

FOF 43) Defendant claims that the July 8, 2009 order authorizing interception of wire communications to and from TT4 violates the particularity requirement of Title III because PTT communications are a separate "facility," yet the order fails to separately identify PTT communications as being subject to interception. (ECF No. 779 at 13-16, 31-32.) The court will address the legal arguments relevant to this challenge in Section III.A.1 and III.B.1., but will summarize the facts pertinent to this challenge here, some of which are dispositive of defendant's legal challenges:

FOF 43(a) When a Nextel cellular telephone device engages in either traditional telephone communications or PTT communications, the same device and the same iDEN network are used. See FOF 3-5, 26-27.

FOF 43(b) A Nextel cellular telephone device cannot engage in either traditional telephone communications or PTT communications without an activated SIM card, which is identified by its IMSI number, inside the device. See FOF 11, 27.

FOF 43(c) A customer cannot engage in PTT communications without using a Nextel cellular telephone device, containing an activated SIM card, and operating on the iDEN network. See FOF 3, 4, 11.

FOF 43(d) Sprint/Nextel uses the IMSI, not the traditional telephone number or UFMI/PTT number, to provision surveillance, and understands that all communications going into and out of that IMSI should be intercepted. See FOF 26.

FOF 43(e) The Attorney General authorized the interception of all wire communications using any telephone number accessed through TT4's IMSI number, including, but not limited to the traditional telephone number (323) 208-0259. See FOF 33.

FOF 44) Defendant claims that the government engaged in unlawful interception of communications occurring over his cellular telephone device, TT4, and other, unidentified, cellular telephone devices, because there are purported anomalies in, and discrepancies between, the data reflected in pen/trap records and CDR. (ECF No. 779 at 18-19; ECF No. 820 at 10-11.) Because the government recounted the content of these allegedly illegally intercepted communications in probable cause affidavits, defendant argues that the resulting warrants were defective, making the resulting searches illegal, warrantless searches. (ECF No. 779 at 5-6.) The record, as a factual matter, contradicts defendant's claims.

FOF 44(a) The record does not support a finding that the government altered pen/trap data before producing it to defendant. Defendant's only evidence in support of this claim is his expert witness' testimony that certain columns were missing from the pen/trap records, and that none of the Sprint/Nextel representatives recognized the format in which the government produced the pen/trap data to defendant. (ECF No. 779 at 6; Gov. Ex. 18 at 17.) Defendant's expert witness never worked in an FBI wire room to observe how surveillance data comes through law enforcement's computer systems, and never implemented a pen/trap order on behalf of a cellular provider. (ECF No. 556 at 35-37; 822 at 60-61; 10-021, ECF No. 164 at 84-85.) Defendant's expert witness was unaware that ASN.1 was a form of computer code in which pen/trap data is delivered to law enforcement and that data could appear in

different formats depending on which service provider is sending the data to law enforcement. (ECF No. 756 at 19-21; Gov. Ex. 18 at 17.) The Sprint/Nextel witnesses explained that they do not create or retain a hard copy of the data pushed to law enforcement, and would not know what it looked like when viewed by law enforcement. (ECF No. 537 at 139-40; ECF No. 756 at 16-21; ECF No. 821 at 133-34; 10-021, ECF No. 164 at 83-84.) There is no support, on this record, for a finding that the government altered pen/trap data before producing it to defendant.

FOF 44(b) The record contradicts defendant's assertion that he never engaged in PTT communications with Blackwell on TT4. (ECF No. 779 at 6 & n.39, 16-17 & n.4.124, 127.) The UFMI/PTT and IMSI numbers associated with defendant's cellular telephone device appear in TT4's pen/trap data many times. (Def. Ex. U; Gov. Ex. 31.) There is no dispute in this record that defendant engaged in PTT communications using his cellular telephone device (identified by IMSI number ending in -0612) with Blackwell, who was using TT4.

FOF 44(c) The record contradicts defendant's assertion that various PTT communications, some of which occurred on July 13 and 16, 2009, and are quoted in probable cause affidavits, were intercepted illegally because they do not appear in the pen/trap records for either defendant's cellular telephone device or TT4. (ECF No. 779 at 23, 31-32; ECF No. 820 at 12-17.)

FOF 44(c)(1) Communications will not appear in pen/trap data if the user is placing an outgoing call in a market that has not been activated or provisioned for surveillance. See FOF 19. Therefore, the absence of a communication from a

pen/trap record is not, standing alone, probative of illegal government interception.

FOF 44(c)(2) Some of the July 16, 2009 communications that are allegedly absent from TT4's pen/trap data occurred before the pen/trap records offered as an exhibit begin. (ECF No. 779 at 23; Def. Ex. U.) The first entry on the pen/trap data for TT4 occurs at 11:35 a.m. on July 16, 2009. (Def. Ex. U.) The absence of communications occurring before 11:35 a.m. on that date is, therefore, not probative of government misconduct.

FOF 44(c)(3) Certain July 16, 2009 communications that are recounted in the probable cause affidavit filed in support of obtaining a search warrant for defendant's tractor truck, (ECF No. 313-5), do appear in the pen/trap records. For example, with time differences and asynchronous clocks accounted for, the communication marked as 99 on Gov. Ex. 31 corresponds to the conversation recounted in paragraph 35 of SA Kopp's affidavit. See FOF 14; (Compare, ECF No. 313-5 and Gov. Ex. 31.) Similarly, the communication marked 83 corresponds to the conversation recounted in paragraph 31 of the affidavit. (Id.) The communications marked 103 and 104 correspond to the conversation recounted in paragraph 37 of the affidavit. (Id.)

FOF 44(c)(4) The July 13, 2009 PTT communication that is recounted in the probable cause affidavit submitted in support of an order authorizing a pen/trap on defendant's cellular telephone device, (Gov. Ex. 1/Def. Ex. E), occurred before the pen/trap records offered as an exhibit begin. (ECF No. 779 at 23.) The pen/trap records upon which defendant relies to support his argument that the



government intercepted that communication using an illegal device, such as a triggerfish or stingray, do not reflect data until July 16, 2009. (ECF No. 779 at 6 & n. 45, 7 & nn. 61-62, 8 & n.70, 16-17 & n. 127; Def. Exs. U (first entry 7/16/09) and V (first entry 7/28/09).) The absence of a July 13, 2009 communication from records that do not begin to reflect data until July 16, 2009 is not probative of government misconduct.

FOF 44(d) The record does not support defendant's assertion that the failure of the CDR for his cellular telephone and TT4 to match the pen/trap records establishes that the government was engaged in illegal surveillance. (ECF No. 779 at 23; ECF No. 822 at 85.) The expert witness who offered this opinion on defendant's behalf did not address the different events recorded by CDR and pen/traps, the asynchronous clocks, different systems and different personnel used to record the data by each system, or the fact that a pen/trap must be activated in a particular market to collect data on outgoing calls. See FOF 14; (ECF No. 756 at 14-15, 113-14; ECF No. 821 at 13.) The expert witness, instead, opined that pen/trap records should be identical to CDR, which opinion is directly contradicted by the testimony of every other witness to address that issue. (10-21, ECF No. 164 at 63, 86.) Moreover, the government demonstrated, by way of reference to defendant's own exhibits, that the pen/trap and CDR do match. (ECF No. 808 at 31-32; Gov. Ex. 31.) Under these circumstances, even if there are discrepancies between the CDR and the pen/trap records, they are not probative of government misconduct because witnesses have offered credible explanations with respect to why these two kinds of records would differ, which defendant did not refute.

FOF 44(e) The record contradicts defendant's assertion that the government used an illegal cell site simulator or digital analyzer (such as a triggerfish or string ray) to intercept communications from his, or Blackwell's, cellular telephone device and pass them on to the Sprint/Nextel network. The Sprint/Nextel representatives were unfamiliar with any device that could accomplish such a task. (ECF No. 756 at 37-39, 64; ECF No. 821 at 115-16.) Defendant's expert witness admitted that for such a device to perform that function, the government would have to follow defendant around the country so that the device would remain physically close to defendant at all times. (09-273, ECF No. 756 at 33; 10-021, ECF No. 164 at 93-94.) The record does not support a finding that the government engaged in such conduct in this case.

FOF 44(f) The record contradicts defendant's assertion that the government illegally gathered information from his cellular telephone device because it knew his whereabouts before July 16, 2009, when the surveillance on his phone began, and knew what markets to activate the pen/trap in by that date. (ECF No. 779 at 7; Gov. Ex. 28.) The record reflects that prior to July 16, 2009, the government was lawfully intercepting the content of conversations occurring on TT4, some of which defendant participated in, for approximately a week, had been gathering data about the usage of TT4 since May 26, 2009, and had been investigating this suspected nationwide drug conspiracy using techniques such as physical surveillance and consulting flight records, all of which had revealed the locus and movements of the conspiracy. (ECF No. 640 at 43, 61, 72-73, 84-85; Def. Ex. PP.) These methods provided the

government with ample information to determine defendant's whereabouts and travels.

FOF 44(g) Because none of defendant's factual claims are supported by the record, there is no basis on which to find that the government used any kind of illegal device to intercept the content of defendant's cellular telephone communications or to track his location.

FOF 45) Defendant claims that the government illegally pinged his cellular telephone device between August 14 and August 18, 2009, as evidenced by the appearance of telephone numbers with the prefix 600 and an internet protocol ("IP") address on the pen/trap records for his cellular telephone device, and SA Evanina's alleged admission to that effect in a probable cause affidavit. (ECF No. 779 at 8-9.) The record, as a factual matter, does not support defendant's claims.

FOF 45(a) The government's first court order to ping defendant's cellular telephone device, (Gov. Ex. 2), expired on August 14, 2009. The government obtained another order to ping defendant's cellular telephone device on August 18, 2009. (Gov. Ex. 3.) Although there was no court order authorizing the pinging of defendant's cellular telephone device in effect between August 14, 2009 and August 18, 2009, defendant's cellular telephone device was still subject to the pen/trap order, which permitted the government to gather contemporaneous cell tower site location information. See FOF 41-42; (ECF No. 537 at 41-44; Gov. Ex. 1.)

FOF 45(b) The record contradicts defendant's contention that traditional telephone numbers bearing the prefix 600 in the pen/trap data indicate that the government was illegally pinging his phone. Sprint/Nextel representatives explained

that the 600 numbers were voice mail notifications that would appear in pen/trap records, but not on CDR. (09-273, ECF No. 821 at 47, 148; 10-021, ECF No. 164 at 170.) Defendant's expert witness could not refute this explanation. (10-021, ECF No. 164 at 96, 97.) SA Maier corroborated this explanation by testifying that she routinely sees the prefix 600 in the pen/trap data for other cases on which she has worked as an FBI agent. (ECF No. 821 at 34.) The record does not support a finding that the 600 numbers indicate that the government was pinging defendant's cellular telephone device without a valid court order.

FOF 45(c) The record contradicts defendant's contention that the appearance of an IP address 156.80.43.5 indicates that the government was illegally pinging his cellular telephone device between August 14 and 18, 2009. (ECF No. 779 at 25-26.) The record reflects that the IP address is assigned to a government contractor and is a technical requirement of Sprint/Nextel in order to transfer both wiretap and pen/trap data to law enforcement. (09-273, ECF No. 756 at 32-34, 35; ECF No. 821 at 61, 79; 10-021, ECF No. 164 at 98, see also ECF No. 822 at 21-22 (defendant's expert acknowledging that this IP address is assigned to a government contractor named Booz Allen.) Defendant's expert witness' testimony that this IP address was evidence of unlawful pinging of a cellular telephone device was speculative, unsubstantiated, and contradicted by all other evidence. Therefore, it is assigned no weight by this court. (10-021, ECF No. 164 at 98-100.) The record does not support a finding that the IP address indicates that the government was illegally pinging defendant's cellular telephone device without a valid court order.

FOF 45(d) The record contradicts defendant's contention that a statement made by SA Evanina in the probable cause affidavit proffered in support of obtaining the second order to ping defendant's cellular telephone device proves that the government was illegally pinging his device between August 14 and 18, 2009. (ECF No. 779 at 8.) The affidavit, which was submitted on August 18, 2009, states that "ping technology also revealed that House remained in California until August 16, 2009 when his cellular telephone was hitting off or signaling off a cell tower in the state of Arizona," indicating that that he was moving East. (Gov. Ex. 3 at 30.)

FOF 45(d)(1) SA Evanina testified that her use of the phrase "ping technology" was an error, and that she should have instead referred to "contemporaneous cell site data for what cell tower the phone was hitting off," which information was still authorized by the sixty-day pen/trap order signed by Magistrate Judge Mitchell on July 16, 2009. (Gov. Ex. 1; ECF No. 537 at 27-28, 35, 38, 55-56, 59, 65-66, 70-71.) SA Evanina's testimony was credible, supported by the record as a whole, and was not contradicted by defendant.

FOF 45(d)(2) Contemporaneous cell tower data would indicate what cell tower a device is using to initiate and receive communications, which would provide broad information such as the state a device is in. See FOF 15. Pinging would provide law enforcement with the exact location of a cellular telephone device. Pinging would not provide information about the cell towers with which a device is communicating; pinging reveals the precise location of a cellular telephone device by sending a signal to that device. See FOF 16. SA Evanina's statement that defendant's cellular telephone was "hitting off or signaling off" of

certain cell towers indicates that contemporaneous cell tower cite location information, and not pinging, was being used to collect the location data.

FOF 45(d)(3) The documentary evidence indicates that the pen/trap on defendant's cellular telephone device was activated in Southern and Northern California, Phoenix, Arizona, and Pittsburgh and Philadelphia, Pennsylvania, supporting SA Evanina's explanation that law enforcement knew the direction in which defendant was travelling on August 16, 2009 by collecting information about the cell towers with which his cellular telephone device was communicating in California and Arizona at that time. (Gov. Ex. 28.) The government was authorized to collect this data pursuant to the pen/trap order signed by Magistrate Judge Mitchell on July 15, 2009. See FOF 40; (Gov. Ex. 1).

FOF 45(d)(4) There is no basis on this record to find that the government was illegally pinging defendant's cellular telephone based upon SA Evanina's use of the phrase "ping technology."

#### **F. The Search of Defendant's Tractor Truck**

FOF 46) On September 13, 2009, a Sunday, at approximately 4:15 p.m., defendant was arrested in the parking lot of a restaurant in Bedford, Ohio, as he attempted to enter his "powder blue tractor cab." (Def. Ex. LL.)

FOF 47) Agents seized defendant's tractor truck and trailer after his arrest because they believed, based upon the entirety of their investigation, which included observing the vehicle drive to and from the Miles Road location, (See FOF 48), that it contained "a significant amount of drugs." (ECF No. 640 at 60-61, 72-73, 83-90.) To prevent the spoilage of perishable produce located in the trailer, and at defendant's request, the produce was delivered to the

intended recipient on September 13 or 14, 2009, under the watch of FBI agents. (Id.) Although defendant contends that the tractor truck and trailer were detached at the time of his arrest, and in different locations, there is no evidence in the record to support any findings in that respect. (ECF No. 820 at 33-34.) SA Kopp was an arresting officer and in a written report submitted to SA Maier stated that the tractor truck and trailer were attached at the time of defendant's arrest, and testified to that effect as well. (ECF No. 640 at 85-86, 88-90; Def. Exs. LL, TT.)

FOF 48) About an hour and a half before defendant's arrest, agents executed a search warrant at 19810 Miles Road, a garage/warehouse in Cleveland, Ohio. (Def. Ex. TT.) Defendant acknowledges being present at that location about an hour before the search was conducted, and agents observed defendant drive his tractor truck to this location on that day, and on other days during the investigation. (ECF No. 779 at 9; ECF No. 640 at 43, 48, 60-61) Approximately 16 kilograms of cocaine were recovered during the search at 19810 Miles Road. (ECF No. 313-5 at 7; Def. Ex. SS.)

FOF 49) A search of defendant's tractor truck occurred on September 15, 2009, pursuant to a warrant signed by a judge in the Northern District of Ohio on that date. (ECF No. 313-4, -5, -6; ECF No. 770 at 13-15; Def. Ex. MM.) The search located a well-concealed, hidden compartment behind a false wall in the sleeping area of the tractor truck in which 25 kilograms of cocaine and 1 kilogram of heroin, packaged in bricks, and attached to strings and hung over metal posts were found. (Def. Ex. MM; ECF No. 770 at 15, 25-26, 37, 70.)

FOF 50) Agents from the FBI and the Ohio Drug Task Force Officers took commemorative photos of the drugs seized as a result of their investigation. (ECF No. 640 at 37-38.) Defendant alleges that the photographs were taken on September 13, 2009, not September 16, 2009, proving that his tractor truck was searched without a warrant, because signs in the

foreground and background of some photographs bear the date “09/13/09,” the dates on certain FBI logs and forms refer to the drugs as having been seized or acquired by the FBI on September 13, 2009, instead of September 16, 2009, and the memory, or SD, card on which the commemorative photographs were initially stored is no longer available to confirm the date of the photographs. (ECF No. 779 at 10, 28-31; Def. Exs. L, N.) The record evidence, however, contradicts defendant’s factual assertions.

FOF 50(a) Law enforcement agents participating in the search testified credibly and consistently that the tractor truck was searched on September 15, 2009, after a search warrant was obtained. (ECF No. 640 at 35; ECF No. 770 at 13-15, 25-27; Def. Exs. MM, TT.)

FOF 50(b) The record reflects that in the commemorative photographs, which were taken on September 16, 2009, at a state law enforcement facility in Brooklyn Heights, Ohio, the date of “09/13/09” on the signs signified when defendant, and certain co-defendants, were arrested, when the Miles Road warehouse was searched, and when law enforcement took possession of defendant’s tractor truck in which a vast amount of drugs would later be discovered pursuant to a search warrant. (ECF No. 640 at 36-40; ECF No. 770 at 5-9.)

FOF 50(c) The documentary evidence reflects, as a whole, that the search of defendant’s tractor truck took place on September 15, 2009.

FOF 50(c)(1) The FBI’s contemporaneous Evidence Recovery Log, and a corresponding report, indicates that the drugs were removed from defendant’s tractor truck on September 15, 2009. (Def. Exs. MM, TT.)



FOF 50(c)(2) The documentary evidence that defendant produced referring to drugs as having being seized on September 13, 2009, (Def. Exs. L, M, XX), is not probative of defendant's assertion that his tractor truck was searched without a warrant.

FOF 50(c)(2)(i) SA Kopp explained that any statements to the effect that evidence was seized on September 13, 2009 would be correct because the government obtained control and possession over defendant's tractor truck on that date in connection with his arrest. (ECF No. 640 at 79-80.) Documents indicating that cocaine was "acquired" or "taken into custody" on September 13, 2009, are, therefore, not probative of defendant's position that his tractor truck was searched without a warrant. (Def. Ex. XX (form FD-192); Def. Ex. L.)

FOF 50(c)(2)(ii) Defendant's collective exhibit XX, which consists of FD-192 and FD-302 forms and "evidence chain of custody" logs, was not offered into evidence at the hearings on these motions. These documents, therefore, are proffered by defendant without explanation or supporting testimony. Some of these forms refer to drug evidence as having been acquired or seized on September 13, 2009. The court's independent review of the collective exhibit indicates that the forms and logs, although apparently all related to the instant drug conspiracy investigation (i.e., 245C-CV-66101, Operation Gummy Worms), concern approximately ten different packages of

drugs, each designated by different “item” and “barcode” numbers. (Def. Ex. XX (e.g., listing barcodes ending in -208, -209, -210, -211, -272, -273, -274, -276, -533, and -534).) The investigation of this case led to the seizure of large quantities of drugs from various locations throughout the country, including 19810 Miles Road, defendant’s tractor truck, a residence, and a subject who travelled from Cleveland, Ohio to Pittsburgh, Pennsylvania. (ECF No. 770 at 7-9.) Some of the searches leading to the recovery of these drugs were lawfully conducted on September 13, 2009. (Id.) For this reason, the forms and logs, without further explanation, cannot be probative of the alleged fact that defendant’s tractor truck was searched on September 13, 2009, without a search warrant. There is no evidence indicating which, if any, of the drugs listed on the forms and logs were recovered from defendant’s tractor truck.

FOF 50(d) The photographic evidence reflects, as a whole, that the search of defendant’s tractor truck took place on September 15, 2009.

FOF 50(d)(1) There is no dispute that evidentiary photographs taken by law enforcement officers, with a Hitachi camera, indicate that defendant’s tractor truck was searched on September 15, 2009. (ECF No. 770 at 10-11, 14, 20, 27.) Electronic files reflecting the date of September 15, 2009, were made available to defendant and his expert for review, and are not being challenged in these proceedings. (ECF No. 537 at 11-14; ECF No. 601-9; ECF No. 770 at 17-21.)

FOF 50(d)(2) Defendant contends that because the electronic data associated with certain commemorative photographs, taken with a Nikon camera, could not be produced by the government, an inference should be made that his tractor truck was searched on September 13, 2009 without a warrant. (ECF No. 779 at 29-31; Gov. Exs. 14, 15; Def. Ex. N.)

FOF 50(d)(2)(i) Credible evidence contradicts the adverse inference that defendant asks this court to make. Two law enforcement officers, who are standing in one of the commemorative photographs, testified that the photographs were taken on September 16, 2009 at a state law enforcement office. See FOF 50(a) and (b).

FOF 50(d)(2)(ii) There is no basis for this court to impose an adverse inference as a sanction due to government misconduct. There is no indication in the record that the commemorative photographs were intended to be proffered as evidence in this matter. There is no evidence that the government acted wrongfully, recklessly, or wantonly in failing to preserve the memory, or SD, card associated with a camera used to take the commemorative photographs.

### **III. CONCLUSIONS OF LAW**

#### **A. General Legal Principles**

##### **1. Suppression of Evidence – Wiretap Evidence**

COL 1) The suppression of wire communications under Title III is governed by 18 U.S.C. § 2518(10)(a). United States v. Williams, 124 F.3d 411, 426 (3d Cir. 1997). That statute provides for the suppression of wire communications if: (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval. Id. (quoting 18 U.S.C. § 2518(10)(a)).

COL 2) Defendant bears the burden of proof on his motion to suppress wiretap evidence. United States v. Savage, No. 07-550, 2013 WL 1334169, at \*20 n.18 (E.D. Pa. Apr. 2, 2013); United States v. Johnson, No. 08-374, 2012 WL 2370434, at \*3 (W.D. Pa. June 21, 2012); see United States v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995) (stating “general rule” in Fourth Amendment context).

COL 3) “If any party claims that evidence is inadmissible because it was the product of an unlawful act, including unlawful use of a wiretap,” the government’s obligation is simply to “confirm or deny the occurrence of the unlawful act.” United States v. Heilman, 377 F.App’x 157, 184 (3d Cir. 2010).

COL 4) Title III requires that each application for an order authorizing the interception of a wire, oral, or electronic communication, and each order authorizing the same, include a description of the nature and location of the communications facilities with respect to which authority to intercept is sought and of the type of communication sought to be intercepted. 18 U.S.C. § 2518(1)(b) and (4).

COL 5) A wire communication is “made in whole or in part through use of facilities for the transmission of communications by the aid of wire, cable, or other like connection.” 18 U.S.C. § 2510(1). This definition undoubtedly includes communications made to or from cellular telephones using cellular telephone networks. See In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t, 620 F.3d 304, 310 (3d Cir. 2010).

COL 6) The term “facility” is not defined in Title III. See 18 U.S.C. § 2518(1)(b)(ii) (requiring “a particular description of the nature and location of the *facilities from which or the place where* the communication is to be intercepted”); § 2518(4)(b) (requiring the order to specify “the communications facilities as to which, or the place where, authority to intercept is granted”).

COL 7) Differences in the statutory text make any definition ascribed to the term “facility” in the Stored Communications Act inapposite. A facility under the SCA is something through which a communication service is provided to multiple users. 18 U.S.C. § 2701(a)(1); In re iPhone Application Litig., 844 F.Supp.2d 1040, 1057 (N.D. Cal. 2012). A facility under the Wiretap Act is something from which or as to which a communication occurs. 18 U.S.C. §§ 2518(1)(b)(ii) and (4)(b).

COL 8) “In the wiretap context, [the Fourth Amendment's particularity] requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized.” United States v. Donovan, 429 U.S. 413, 427 n.15 (1977).

COL 9) The Supreme Court has never “go[ne] so far as to suggest that every failure to comply fully with any requirement provided in Title III would render the interception of wire or oral communications ‘unlawful.’” United States v. Chavez, 416 U.S. 562, 574-75 (1974). Minor,

technical violations do not require suppression. United States v. Mainor, 393 F.App'x 10, 15 (3d Cir. 2010) (“[E]very circuit to consider the question has held that § 2518(10)(a)(ii) does not require suppression if the facial insufficiency of the wiretap order is no more than a technical defect.”) (internal quotation marks and citation omitted). Suppression is mandated only “where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” United States v. Giordano, 416 U.S. 505, 527 (1974) (suppression of wiretap evidence was warranted where the government failed to obtain authorization from the attorney general, or other official, before applying for wiretap order; that requirement was fundamental and not technical). Statutory violations that would have precluded a court from authorizing the wiretap in the first instance are those that require suppression. Donovan, 429 U.S. at 433-36 & n.24 (while the complete absence of prior judicial authorization would make a wiretap unlawful, a technical violation of Title III (e.g., failing to identify every individual who could be expected to be overheard), would not).

COL 10) Although there is no binding legal authority with respect to whether intercepted PTT communications must be suppressed where the wiretap application or order fail to explicitly specify the UFMI/PTT number, general legal principles applicable to Title III, and analogous case law, are instructive.

COL 10(a) Defendant did not cite legal authority from any jurisdiction finding that Title III's requirement that the facility be identified with particularity is violated if the UFMI/PTT number is not specified in the affidavit, application, and court orders.

COL 10(b) In United States v. Vasconcellos, the district court, interpreting a New York statute analogous to Title III, held that identification of the traditional telephone

number and subscriber information was sufficient to satisfy equivalent particularity requirements set forth in that statute with respect to the interception of PTT communications. United States v. Vasconcellos, 658 F. Supp. 2d 366, 394 (N.D.N.Y. 2009).

COL 10(c) Cellular telephone devices are sufficiently identified for purposes of Title III by IMSI or ESN number, subscriber information, traditional telephone number, or UFMI/PTT number, or any combination of the same.

COL 10(c)(1) “Although the ‘nature and location’ of a cellular phone cannot be described in the same way as that of a land line phone, a cellular phone is itself a ‘facilit[y]’ that can be sufficiently identified by such features as its telephone number, electronic serial number (ESN) or international mobile subscriber identity number (IMSI).” United States v. Oliva, 705 F.3d 390, 396 n.4 (9th Cir. 2012). A wiretap order may be valid even if it includes only one of the three possible identifiers. United States v. Duran, 189 F.3d 1071, 1086 (9th Cir. 1999).

COL 10(c)(2) A cellular telephone is a facility that is sufficiently identified by the ESN and traditional telephone number. United States v. Goodwin, 141 F.3d 394, 403 (2d Cir. 1997). An order authorizing interception “provides more than adequate particularity to identify the cellular telephone over which the intercept is authorized” where it identified both the IMSI and traditional telephone number. United States v. Flores, No. 105-558, 2007 WL 2904109, at \*18 (N.D. Ga. Sept. 27, 2007). Even if the ESN number is not listed, where subscriber information and traditional telephone numbers have been listed a

cellular telephone device is sufficiently identified. United States v. Ortiz, No. 12-0119, 2013 WL 6842537, at \*4 (N.D. Cal. Dec. 27, 2013).

COL 10(c)(3) Interception can continue, and the particularity requirement still be met, if the identifying numbers (i.e., the ESN or IMSI) are changed, or the associated traditional telephone number is changed, even if the court order does not specify that interception can continue in those circumstances. United States v. Jackson, 41 F.App'x 848, 851 (7th Cir. 2002); United States v. Brown, 41 F.App'x 866, 868-69 (7th Cir. 2002) (same); United States v. Duran, 189 F.3d 1071 (9th Cir. 1999); United States v. Banks, No. 13-cr-40060, 2014 WL 5321075, at \*5 (D. Kan. Oct. 17, 2014); Flores, 2007 WL 2904109, at \*18 (collecting decisions in which particularity requirement of Title III was met by identifying traditional telephone number and ESN, and providing for continued interception even if those numbers were changed).

COL 11) Suppression may still not be warranted where law enforcement agents rely in good faith on a judicially authorized wiretap order. United States v. Kaplan, No. 06-719, 2009 WL 3806277, at \*18 (E.D. Pa. Nov. 13, 2009) (noting that the Court of Appeals for the Third Circuit has not yet decided whether the good faith exception applies in the context of wiretaps, and collecting decisions reflecting circuit split). Under the good-faith exception “evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant” should not be suppressed. United States v. Wright, 777 F.3d 635, 638 (3d Cir. 2015).



## **2. Suppression of Evidence – Pinging Evidence**

COL 12) Neither the United States Supreme Court, nor the Court of Appeals for the Third Circuit, has decided whether individuals have a reasonable expectation of privacy in the real-time cellular telephone location data that is collected when a cellular telephone is “pinged.” In re Application of the U.S. for an Order for Authorization to obtain Location Data Concerning an AT & T Cellular Tel., No. 3:15-MC-3, 2015 WL 1842761, at \*1-10 (N.D. Miss. Mar. 30, 2015) (summarizing the current state of the law, and the potentially applicable statutes and federal rules under which ping orders may be obtained); see also State of Missouri v. Hosier, 454 S.W.3d 883, 897 (Mo. 2015) (same).

## **3. Suppression of Evidence – Search of Defendant’s Tractor Truck**

COL 13) The Fourth Amendment prohibits “unreasonable searches and seizures” of “persons, houses, papers, and effects.” U.S. Const. amend. IV.

COL 14) The Fourth Amendment generally requires police to secure a warrant supported by probable cause before conducting a search, unless a recognized exception to the warrant requirement exists. Maryland v. Dyson, 527 U.S. 465, 466 (1999) (citing California v. Carney, 471 U.S. 386, 390-91 (1985)). Warrantless searches are presumptively unreasonable, subject to certain specifically established and well-delineated exceptions. Horton v. California, 496 U.S. 128, 133 (1990).

COL 15) In the context of a motion to suppress evidence obtained in connection with a warrantless search, the government bears the burden to prove by a preponderance of the evidence that the disputed search falls within one of the recognized exceptions to the warrant requirement. United States v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995); United States v. Herrold, 962 F.2d 1131, 1137 (3d Cir. 1992).

COL 16) Any evidence obtained in connection with an illegal search must be suppressed as “fruit of the poisonous tree.” United States v. Brown, 448 F.3d 239, 244 (3d Cir. 2006) (citing Wong Sun v. United States, 371 U.S. 471, 487–88 (1963)).

COL 17) The search incident to arrest exception permits vehicle searches only “if it is ‘reasonable to believe [that] evidence relevant to the crime of arrest might be found.’” United States v. Donahue, 764 F.3d 293, 300 n.6 (3d Cir. 2014) (quoting Arizona v. Grant, 556 U.S. 332, 335 (2009)). The exception requires “a lesser basis for a search than a showing of probable cause,” but authorizes searches only for evidence related to the crime prompting the arrest, not to evidence of other offenses. Id. (citations omitted).

COL 18) The automobile exception permits “the search of every part of the vehicle and its contents that may conceal the object of the search” provided that probable cause supports such search. Id. at 300 (citation omitted). The validity of a search pursuant to the automobile exception depends upon whether the officers had probable cause to believe that the seized vehicle contained, at the time of the search, evidence of a crime. Id. at 301.

#### **4. Franks Hearing**

COL 19) In Franks v. Delaware, the Supreme Court held that a defendant may challenge the presumed validity of an affidavit of probable cause used to secure a search warrant by attacking the truthfulness of the factual statements made in the affidavit. Franks v. Delaware, 438 U.S. 154, 155-56 (1978). When appropriate, the court will hold a Franks hearing to give the defendant an opportunity to present evidence which challenges the truthfulness of the affidavit. United States v. Yusuf, 461 F.3d 374, 383 (3d Cir. 2006).

COL 20) In order to obtain a Franks hearing, a defendant must first make a “substantial preliminary showing” that: (a) the affidavit contained a false statement, which was made

knowingly or with reckless disregard for the truth that (b) is material to the finding of probable cause. Yusuf, 461 F.3d at 383. To make a substantial preliminary showing, “the defendant cannot rest on mere conclusory allegations or a mere desire to cross-examine, but rather must present an offer of proof contradicting the affidavit, including materials such as sworn affidavits or otherwise reliable statements from witnesses.” Id. at 383 n.8 (internal quotations omitted).

COL 21) To determine whether the deficiencies in the affidavit are “material” to the determination of probable cause, the court must follow the following procedure: when faced with an affirmative misrepresentation, the court is required to excise the false statement from the affidavit. In contrast, when faced with an omission, the court must remove the “falsehood created by an omission by supplying the omitted information to the original affidavit.” Id. at 384. If probable cause still exists after the affidavit has been “corrected,” then the deficiencies are not material. Id.

COL 22) Franks hearings are also appropriate when a defendant is challenging statements or omissions contained in applications for the interception of oral, wire, and electronic communications under Title III. United States v. Heilman, 377 F.App’x 157, 177 (3d Cir. 2010).

COL 23) If the defendant meets this burden and a hearing is granted, the defendant must prove by a preponderance of the evidence that: (a) the affiant knowingly and deliberately, or with a reckless disregard for the truth, made false statements or omissions that create a falsehood in applying for a warrant; and (b) such statements or omissions were material, or necessary, to the probable cause determination. Id. at 383. Under the Franks standard, to prove the affiant acted with a reckless disregard for the truth, the defendant must show “the affiant must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the

accuracy of the information he reported.” United States v. Brown, 631 F.3d 638, 645 (3d Cir. 2011) (quoting Wilson v. Russo, 212 F.3d 781, 788 (3d Cir. 2000)).

## **5. Dismissal of the Indictments**

COL 24) The Due Process Clause of the Fifth Amendment is violated when law enforcement officers engage in outrageous misconduct in detecting and obtaining incriminating evidence. Rochin v. California, 342 U.S. 165 (1952). When government misconduct is found to violate the Fifth Amendment, the indictment must be dismissed because the government conduct is deemed to render “the prosecution of the defendant fundamentally unfair.” United States v. Lakhani, 480 F.3d 171, 181 (3d Cir. 2007).

COL 25) Dismissal of an indictment may only be ordered in narrow circumstances and upon a finding of willful prosecutorial misconduct which violates the Due Process Clause and causes prejudice to the defendant. Gov't of Virgin Islands v. Fahie, 419 F.3d 249, 255 (3d Cir. 2005); see United States v. Lashley, 524 F.App'x 843, 846 (3d Cir. 2013). Willful prosecutorial misconduct may be demonstrated through “a constitutional violation that results from a reckless disregard for a defendant's constitutional rights,” or a pattern of constitutional violations showing recklessness on behalf of the prosecution. Fahie, 419 F.3d at 255–56. The Court of Appeals for the Third Circuit has recognized that “the challenged conduct must be shocking, outrageous, and clearly intolerable” and that “this is an extraordinary defense reserved for only the most egregious circumstances.” United States v. Nolan–Cooper, 155 F.3d 221, 230–31 (3d Cir. 1998) (internal citations omitted).

COL 26) Federal Rule of Criminal Procedure 16 requires the government to disclose certain specified categories of evidence to a defendant upon request. FED.R.CIV.P. 16.

COL 27) The Brady doctrine requires the government to disclose exculpatory evidence to defendant. To prove a Brady violation, the defendant must show that “(1) the government withheld evidence, either willfully or inadvertently; (2) the evidence was favorable, either because it was exculpatory or of impeachment value; and (3) the withheld evidence was material.” Lambert v. Blackwell, 387 F.3d 210, 252 (3d Cir. 2004). “Evidence is ‘material’ where there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A ‘reasonable probability’ is a probability sufficient to undermine confidence in the outcome.” Maynard v. Gov’t of Virgin Islands, 392 F.App’x 105, 112 (3d Cir. 2010).

COL 28) A court may not dismiss an indictment as a sanction for either a Brady violation, or a Rule 16 violation unless the court finds both prejudice to the defendant and willful misconduct by the Government. United States v. Hastings, 461 U.S. 499 (1983); Fahie, 419 F.3d at 259.

COL 29) Rule 48(b) of the Federal Rules of Criminal Procedure permits a court to dismiss an indictment if unnecessary delay occurs in bringing a defendant to trial. FED.R.CIV.P. 48(b)(3). Rule 48(b) is a codification of a court’s “inherent power to dismiss a case simply for want of prosecution” and applies to situations in which the Speedy Trial Act has not necessarily been violated. United States v. Dreyer, 533 F.2d 112, 113 n.1 (3d Cir. 1976).

COL 30) The district court’s decision to grant or deny a Rule 48(b) motion is discretionary. Gov’t of Virgin Islands v. Lee, 775 F.2d 514, 526 (3d Cir. 1985). In exercising this discretion, a court is to consider: (1) the length of delay; (2) the reason for the delay; (3) the defendant’s assertion of his right; and (4) prejudice to the defendant. Barker v. Wingo, 407 U.S. 514, 530 (1972).

## **B. Analysis and Conclusions**

### **1. Suppression of PTT Communications to and from TT4**

COL 31) The content of PTT communications to and from TT4 will not be suppressed on the ground that the Attorney General's July 7, 2009 authorization, and Judge Cercone's July 8, 2009 order did not include a UFMI/PTT number. There is no legal requirement that PTT communications be separately identified from traditional telephone communications, and, even if there were, the requirement would be technical, thus not warranting suppression, and the agents would be able to invoke the good faith exception in any event.

COL 32) The Authorization for Interception Order Memorandum issued by the Attorney General's Office on July 7, 2009, (Def. Ex. YY), complied with all requirements of Title III and authorized the interception of PTT communications to and from TT4, including those in which defendant participated.

COL 33) The Authorization identified the type of communication as "wire communications," as opposed to oral or electronic communications, listed the traditional telephone number, subscriber information, and IMSI number associated with TT4, authorized the interception of any wire communications accessed through the IMSI number, permitted the interception of communications occurring over changed telephone or IMSI numbers, and was signed by an authorized designee of the Attorney General's Office. See FOF 33.

COL 34) Defendant's legal challenge to the validity of this Authorization on the ground that it does not include a UFMI/PTT number, or specify that PTT communications can be intercepted fails for the same reasons that defendant's challenge to the July 8, 2009 wiretap order on that legal basis fails. Conclusions of Law 35 through 37(e), are fully incorporated herein.

COL 35) The wiretap order, signed by Judge Cercone on July 8, 2009, (Def. Ex. C), complied with all requirements of Title III, and authorized the interception of PTT communications to and from TT4, including those in which defendant participated. See FOF 32.

COL 36) The order included a sufficient description of the nature and location of the communications facilities with respect to which authority to intercept was sought and of the type of communication sought to be intercepted. The order identified the type of communication as “wire communications,” as opposed to oral or electronic communications. See FOF 32. The order identified the facilities with respect to which authority to intercept was sought by listing the IMSI number, subscriber information, and the traditional telephone number associated with that device. See FOF 32; 18 U.S.C. § 2518(1)(b) and (4). The order stated that interception could continue even if either the IMSI number or traditional phone number was changed. See FOF 32.

COL 37) There is no requirement that the UFMI/PTT number be separately identified in an order authorizing the interception of wire communications from a cellular telephone device to permit the interception of PTT communications, as well as traditional telephone communications, to and from that device.

COL 37(a) No binding or persuasive legal authority has held that traditional telephone communications and PTT communications to and from the same cellular telephone device are different “facilities” within the meaning of Title III. Decisions interpreting the SCA are not persuasive, or even instructive. COL 10 and 10(a).

COL 37(b) No binding legal authority states that Title III requires a UFMI/PTT number to be separately identified in order for a wiretap order to authorize the interception of PTT communications. COL 10 and 10(a).

COL 37(c) No persuasive legal authority states that Title III requires a UFM/PTT number to be separately identified in order for a wiretap order to authorize the interception of PTT communications. To the contrary, the most analogous decision that this court reviewed held, under a state law analogous to Title III, that that identification of the traditional telephone number and subscriber information was sufficient to satisfy particularity requirements such that PTT communications could be lawfully intercepted. COL 10(b).

COL 37(d) Analogous case law indicates that cellular telephone devices are sufficiently identified by IMSI number, ESN number, the subscriber information, traditional telephone number, UFM/PTT number, or any combination of the same. COL 10(c) and 10(c)(1) – (c)(3).

COL 37(e) The court concludes that PTT communications to and from TT4 were identified in conformance with the particularity requirements of Title III because: (a) the IMSI number, subscriber information, and traditional telephone number were provided; (b) the interception of wire communications using a different telephone number was specifically permitted; (c) the same IMSI number and the same iDEN network were used to engaged in traditional telephone and PTT communications to and from TT4; (d) TT4 could not be used to engage in PTT communications unless a SIM card, containing the IMSI number, was inserted into the device; and (e) the IMSI number is sufficient to enable Sprint/Nextel, from a technological standpoint, to provision a wiretap to intercept both traditional and PTT communications. See FOF 3-5, 26-27, 32-38, 43 (including all subparts); COL 10 (including all subparts).



COL 38) Even if Title III required the identification of the UFMI/PTT number, suppression of PTT communications to and from TT4 would not be warranted. The inclusion of this additional identifying information does not directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device and does not equate to an absence of prior judicial authorization. COL 9. The absence of the UFMI/PTT would, instead, be a minor, technical violation that would not have prevented the judicial officer from issuing the wiretap order in the first instance. COL 9.

COL 39) Even if the July 8, 2009 wiretap order were deemed defective and unlawful because it failed to include a UFMI/PTT number, suppression of PTT communications to and from TT4 would not be warranted because the law enforcement agents reasonably relied in good faith on that judicially authorized wiretap order. COL 11. The court order appears valid on its face, contains information sufficient to allow law enforcement and cellular service providers to identify TT4, and no established legal authority requiring the UFMI/PTT number to be included in the order existed in 2009 (or exists now). COL 11.

COL 40) The wiretap evidence acquired from TT4 will not be suppressed on the ground that the government used an unlawful device or method to intercept the content of communications because there is no factual support for the numerous arguments that defendant makes in support of his motion to suppress in this respect. See FOF 44 (including all subparts) and FOF 45 (including all subparts).

COL 41) The government produced credible evidence with respect to why CDR and pen/trap data would contain discrepancies. See FOF 44(c) (including all subparts) and FOF 44(d). Defendant's expert witness failed to account for these explanations, and his testimony

that the CDR and pen/trap data would be identical was not credible and was disproven by undisputable evidence, such as, for example, that different systems, with different clocks are used to create the two kinds of records, different network events trigger an entry in each record, and that pen/traps and wiretaps will only collect information about outgoing communications when the user is in a market that has been provisioned or activated for surveillance. See FOF 14, 17, 19, 44(c)(1), 44(d).

COL 42) The documentary evidence establishes that defendant communicated with Blackwell on TT4, even though defendant contends that he only communicated with Blackwell using a different, unidentified, cellular telephone device. See FOF 44(b).

COL 43) The government demonstrated, by way of example, that various communications, the content of which were recounted in probable cause affidavits, are reflected in the pen/trap records, contrary to defendant's assertion that they are not. See FOF 44(c)(3).

## **2. Suppression of Location Evidence related to Defendant's Cellular Telephone**

COL 44) The location surveillance evidence acquired from defendant's cellular telephone device will not be suppressed on the ground that the government used an unlawful method or device to ping defendant's cellular telephone device between August 14, 2009 and August 18, 2009, because there is no factual support for the arguments that defendant makes in support of his motion to suppress in this regard. See FOF 45 (including all subparts).

COL 45) The lack of consensus with respect to the legal standard that must be met in order to obtain a court order to ping a cellular telephone device is not germane to defendant's motion because defendant's challenges are factual, not legal. See FOF 45; COL 12. Defendant makes no claim that the government failed to make the requisite showing in order to obtain the ping orders that were signed by Magistrate Judges Mitchell and Lenihan.

COL 46) The government produced credible evidence with respect to the appearance of entries in the pen/trap with the prefix 600 and the identified IP address. See FOF 45 and 45(a) – (d). Defendant’s expert witness’ testimony that these numbers were evidence of unlawful pinging of a cellular telephone device was unsubstantiated, and not credible. See FOF 45(b) and (c).

COL 47) The government produced credible evidence with respect to SA Evanina’s misuse of the term “pinging technology” in the affidavit she submitted in order to obtain a second court order to ping defendant’s cellular telephone device. See FOF 45(d) (including all subparts). Defendant presented no evidence contradicting SA Evanina’s explanation, or impeaching her testimony. The record reflects that contemporaneous cell tower site location data was used to determine that defendant was travelling east from California on August 16, 2009, and that the collection of that data was authorized by the pen/trap order on defendant’s cellular telephone device, which was lawful and still in effect on that date. See FOF 40; FOF 45(a); and FOF 45(d) (including all subparts).

### **3. Suppression of Evidence Obtained from the Search of Defendant’s Tractor Truck**

COL 48) The search of defendant’s tractor truck was a lawful search, conducted pursuant to a warrant, on September 15, 2009. See FOF 49, 50, 50(a), 50(c) (including all subparts), 50(d) (including all subparts).

COL 49) The inability of the government to produce the memory, or SD, card used to take commemorative photographs, and government documents indicating that drugs were seized or acquired on September 13, 2009, are not probative that a warrantless search occurred. See FOF 50(d)(2) (including all subparts) and 50(d) (including all subparts).

COL 50) Even if the search was conducted on September 13, 2009, prior to issuance of a search warrant, the search would have been lawful, and suppression of the drug evidence seized would not be necessary, because the government proved, by a preponderance of the evidence, that the arresting officer possessed both a reasonable belief at the time that evidence relevant to the crime of arrest could be found in the tractor truck and probable cause to believe that the tractor truck contained evidence of a crime. See FOF 2, 46-48; COL 17-18.

#### **4. Franks Hearing**

COL 51) Defendant is not entitled to a Franks hearing with respect to the warrant issued by the federal district court in Ohio on September 15, 2009, to search defendant's tractor truck, on the ground that the truck had already been illegally searched on September 13, 2009. (ECF No. 779 at 27-45; ECF No. 820 at 10-19, 23-30, and 38-39.) Defendant cannot make a "substantial preliminary showing" that the affidavit submitted to the court in Ohio contained false statements about when his tractor truck was searched for all the reasons set forth above. The record contradicts defendant's factual assertion that his tractor truck was illegally searched on September 13, 2009, without a warrant. See FOF 46-50 (including all subparts); COL 48-50.

COL 52) Defendant is not entitled to a Franks hearing with respect to affidavits filed in support of obtaining orders to ping and to install a pen/trap on his cellular telephone device, and to continue the interception of wire communications to and from TT4 on the ground that the government intercepted PTT communications without authorization from the Attorney General, or a court order, or by using an illegal device, such as a string ray or triggerfish to intercept PTT communications to and from TT4. (Gov. Exs. 1-3; Def. Ex. D; ECF No. 779 at 27-45; ECF No. 820 at 10-19, 23-30, and 38-39.) Defendant cannot make a "substantial preliminary showing" that the affidavits contained false statements about the circumstances under which the content of

PTT communications were intercepted, for all the reasons set forth above. The record contradicts defendant's factual assertion that the government illegally intercepted his communications. See FOF 43-45 (including all subparts); COL 31-47 (including all subparts).

COL 53) Defendant is not entitled to a Franks hearing with respect to the affidavit filed by SA Evanina in support of obtaining the second order to ping his cellular telephone device on the ground that the government used an illegal device to ping his cellular telephone device between August 14, 2009 and August 18, 2009. (Gov. Ex. 3; Def. Ex. D; ECF No. 779 at 27-45; ECF No. 820 at 10-19, 23-30, and 38-39.) Defendant cannot make a "substantial preliminary showing" that the affidavit contained false statements about how his location was determined on August 16, 2009, for all the reasons set forth above. See FOF 42, 45 (including all subparts); COL 44-47 (including all subparts).

COL 54) Because defendant failed to establish by competent evidence that a false statement was made, the question of materiality is irrelevant.

COL 55) In any event, during the numerous hearings in these proceedings defendant was given the opportunity to cross-examine affiants SA Evanina, SA Maier, and SA Kopp, which provided defendant with the opportunity to gather evidence to prove, by a preponderance of the evidence, that the affiant knowingly and deliberately, or with a reckless disregard for the truth, made false statements in applying for a warrant. Yusuf, 461 F.3d at 383. Defendant was provided with a de facto Franks hearing. Defendant still, however, presented no evidence in support of his contention that any affiant acted knowingly, deliberately, or with reckless disregard for the truth.

## **5. Dismissal of the Indictments**

COL 56) Defendant is not entitled to dismissal of the indictments under either Rule 16 or the Brady doctrine because defendant did not demonstrate either willful government misconduct, or prejudice.

COL 57) There is no evidence that the government's conduct was shocking, outrageous, or egregious with respect to producing the electronic data associated with the commemorative photographs. The government produced the electronic data associated with the pictures that were taken for evidentiary purposes, and two law enforcement officers who appear in the commemorative photographs testified about when the commemorative photographs were taken. See FOF 50(b) and 50(d) (including all subparts). Defendant produced no evidence indicating that the government acted wrongfully, recklessly, or wantonly in failing to preserve the memory, or SD, card associated with the commemorative photographs. COL 24-28. Dismissal of the indictments, therefore, cannot be justified on this alleged basis.

COL 58) Defendant made no showing that he has been prejudiced by the government's failure to produce electronic data associated with the commemorative photographs. There is no probative evidence in the record to support defendant's contention that his tractor truck was searched on September 13, 2009. See FOF 46-50. Dismissal of the indictments, therefore, cannot be warranted on this alleged basis.

COL 59) Defendant presented no probative evidence that the government altered the pen/trap data before producing it to defendant. See FOF 44(a). It follows that defendant can make no showing of willful, shocking, or outrageous government misconduct, or prejudice, in this respect and that dismissal of the indictments cannot be warranted on this alleged basis. COL 24-28.

COL 60) This court will not exercise the inherent, and discretionary, power to dismiss the indictments in this case under Rule 48(b)(3) because the delay in these proceedings was the result of defendant's numerous motions to suppress and related motions to compel, and the hearings afforded to defendant to prove his contentions. See FOF 1. Defendant was not prejudiced by this delay because it was for the purpose of asserting his rights.

DATED: July 8, 2015

BY THE COURT:

/s/Joy Flowers Conti

Joy Flowers Conti

Chief United States District Judge